

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS**

KIRKSTON SPANN II and ROCHELLE LAMPKIN, *on behalf of themselves and all others similarly situated*,

Plaintiffs,

v.

SUPERIOR AIR-GOUND AMBULANCE SERVICE, INC.,

Defendant.

Case No: 1:24-cv-04704

Judge Matthew F. Kennelly

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Kirkston Spann II and Rochelle Lampkin¹ (“Plaintiffs”) bring this Consolidated Class Action Complaint against Superior Air-Gound Ambulance Service, Inc. (“Defendant”), individually and on behalf of all others similarly situated, and allege—upon personal knowledge as to their own actions and their counsels’ investigation and upon information and belief as to all other matters—as follows:

SUMMARY OF THE ACTION

1. Plaintiffs bring this class action lawsuit against Defendant for its failure to properly secure and safeguard sensitive information of its patients from cybercriminals.
2. Defendant is a corporation that provides ambulance and other healthcare-related travel services and currently has “over 3,000 employees and provide[s] EMS in five states.”²

¹ Due to a typographical error, Plaintiff Rochelle Lampkin’s name was initially spelled incorrectly but it has now been corrected for this Consolidated Complaint.

² <https://www.superiorambulance.com/about-us/>

3. As part of its business, Defendant collected and maintained certain personally identifiable information (“PII”) and protected health information (“PHI”, collectively with PII, “Private Information”) of Plaintiffs and the putative Class Members (defined below), who are (or were) patients of Defendant.

4. Plaintiffs’ and Class Members’ sensitive personal information—which they entrusted to Defendant on the mutual understanding that it would protect it against disclosure—was targeted, compromised and unlawfully accessed due to the data breach on or about May 2023 based on the notice posted in June 2024 (the “Data Breach”).

5. Upon information and belief, the Private Information compromised in the Data Breach included Plaintiffs’ and Class Members’ names, addresses, dates of birth, Social Security numbers, driver’s license or state identification numbers, financial account information and payment cards information as well as medical treatment and health insurance information, which is PHI as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

6. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

7. As a result of the Data Breach, Plaintiffs and approximately 858,000 Class Members³ suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with

³ According to the breach report submitted to the Office of the U.S. Department of Health and Human Services, 858,238 persons were impacted in the Data Breach. See https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs' Private Information being disseminated on the dark web; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' Private Information from a foreseeable and preventable cyber-attack.

9. Moreover, upon information and belief, Defendant was targeted for a cyber-attack due to its status as a healthcare entity that collects and maintains highly valuable Private Information on its systems.

10. Healthcare providers that handle Private Information have an obligation to employ reasonable and necessary data security practices to protect the sensitive, confidential, and personal information entrusted to them.

11. This duty exists because it is foreseeable that the exposure of such Private Information to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, medical and financial identity theft, invasion of their private health matters, and other long-term issues.

12. Defendant maintained, used and shared the Private Information in a reckless manner. In particular, the Private Information was used and transmitted by Defendant in a condition vulnerable to cyberattacks.

13. Upon information and good faith belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

14. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions, failing to take standard and reasonably available steps to prevent the Data Breach, and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

15. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained has been accessed and acquired by data thieves.

16. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

17. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

18. Plaintiffs and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

19. Plaintiffs bring this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

20. Plaintiffs, on behalf of themselves and all others similarly situated, therefore bring claims for (i) negligence, (ii) breach of implied contract, (iii) breach of fiduciary duty; (iv) violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2 *et seq.* ("ICFA"); (v) violation of the Michigan Consumer Protection Act, Mich. Comp. Laws Ann. § 445.901 *et seq.*, and (vi) unjust enrichment. Plaintiffs seek damages and injunctive relief, including the adoption of reasonably necessary and appropriate data security practices to safeguard the Private Information in Defendant's custody to prevent incidents like the Data Breach from occurring in the future.

PARTIES

21. Plaintiff Kirkston Spann II is, and has been at all relevant times, a resident and citizen of Marysville, Indiana.

22. Plaintiff Rochelle Lampkin is, and has been at all relevant times, a resident and citizen of Highland Park, Michigan.

23. Defendant Superior Air-Gound Ambulance Service, Inc. is a corporation organized and existing under the laws of the State of Illinois with its principal place of business located in Elmhurst, Illinois.

JURISDICTION & VENUE

24. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of \$5,000,000 exclusive of interest and costs, and members of the proposed Class, including Plaintiffs, are citizens of states different from Defendant.

25. This Court has jurisdiction over Defendant through its business operations in this District, the specific nature of which occurs in this District. Defendant's principal place of business is in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) through (d) because Defendant's principal place of business is located in this District and a substantial part of the events and omissions giving rise to this action occurred in this District.

COMMON FACTUAL ALLEGATIONS

A. Defendant Collects Its Patients' Private Information.

27. Defendant is a corporation that provides ambulance and other healthcare-related travel services and currently has "over 3,000 employees and provide[s] EMS in five states."⁴

28. Plaintiffs and Class Members are current and former patients at Defendant.

⁴ <https://www.superiorambulance.com/about-us/>

29. As a condition of obtaining services from Defendant, patients and other personnel, such as Plaintiffs, were required to entrust Defendant with their highly sensitive personal information.

30. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiffs, Defendant promised to provide confidentiality and adequate security for the data it collected from patients through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

31. Indeed, Defendant states on its website that: “[y]our health information is personal, and Superior Air-Ground Ambulance Service, Inc., Superior Air-Ground Ambulance Service of Indiana, Inc., Superior Air-Ground Ambulance Service of Michigan, Inc., and Superior Air-Ground Ambulance Service of Ohio, Inc., and Superior Air-Ground Ambulance Service of Wisconsin, Inc., and Superior Air Ambulance Service, Inc. (collectively Superior Ambulance Service) is committed to protecting it. We are required by law to maintain the privacy of your protected health information (PHI) that could be used to identify you. The law also requires us to provide you with a copy of this Notice of Privacy Practices (Notice), which describes our privacy practices and our legal duties with respect to PHI. Under certain circumstances, we may also be required to notify you following a breach of unsecured PHI.”⁵

32. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, Defendant is required to keep patients’ Private Information private, comply with industry standards related to data security and the maintenance of their patients’ Private Information, inform their patients of its legal duties relating to data security, comply with all federal and state laws protecting patients’ Private Information, only use

⁵ <https://www.superiorambulance.com/hippa-privacy-policy-1/>

and release patients' Private Information for reasons that relate to the services they provide, and provide adequate notice to patients if their Private Information is disclosed without authorization.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

34. Plaintiffs and Class Members, as patients of Defendant, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Private Information, especially when their Social Security numbers and other sensitive Private Information is involved.

35. Defendant's actions and inactions directly resulted in the Data Breach and the compromise of Plaintiffs' and Class Members' Private Information

B. The Data Breach.

36. In or about May 2024, Defendant posted a notice to its website (the "Online Notice"), informing Plaintiffs and Class Members that:

What Happened? In May 2023, Superior learned of unusual activity within its computer systems. Superior promptly took steps to secure the system and began a comprehensive investigation to confirm the full nature, scope, and impact of the event. On June 23, 2023, the investigation determined that an unauthorized actor copied certain files from the network between May 15 and May 23, 2023. Superior subsequently worked to undertake a comprehensive and time-intensive review of the affected files to identify and catalogue what information was present and to whom that information relates. Superior then worked to determine contact information for those individuals. Superior is now taking steps to notify potentially affected individuals of this event.

What Information Was Involved? The information that is present in the affected files varies by individual but may include: name, address, date of birth, Social Security numbers, driver's license or state identification number, financial account information, payment card information, patient record information, medical diagnosis or condition information, medical treatment information, and health insurance information.⁶

37. Omitted from the Online Notice was the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

38. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach’s critical facts. Without these details, Plaintiffs’ and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

39. Despite Defendant’s intentional opacity about the root cause of this incident, several facts may be gleaned from the Online Notice, including: (i) that this Data Breach was the work of cybercriminals; (ii) that the cybercriminals first infiltrated Defendant’s networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson’s terms “stole” data; and (iii) that once inside Defendant’s networks and systems, the cybercriminals targeted information including, upon information and belief, Plaintiffs’ and Class Members’ PHI, PII, and other sensitive information for download and theft.

40. Moreover, in its Online Notice, Defendant failed to specify whether it undertook any efforts to contact the approximate 858,000 Class Members whose data was accessed and

⁶ The “Online Notice”. A sample copy is available at <https://about.Defendant.org/news/2024/05/network-interruption-update>

acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data or whether Defendant was interested in hearing about misuse of their data or set up a mechanism for Class Members to report misuse of their data.

41. Defendant had obligations created by the FTC Act, HIPAA, contract, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

42. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

43. The attacker accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

44. Plaintiff Spann II has been informed by Credit Karma that his Private Information has been disseminated on the dark web.

45. Plaintiffs further believe that the Private Information of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

46. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the breach.

C. Defendant Knew, or Should Have Known, of the Risk of Storing Valuable Private Information & the Foreseeable Harm.

47. Defendant was well aware that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

48. Defendant also knew that a breach of its systems—and exposure of the information stored therein—would result in the increased risk of identity theft and fraud (financial and medical) against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

49. These risks are not merely theoretical; in recent years, numerous high-profile data breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem as well as countless ones in the healthcare industry.

50. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.⁷

51. The healthcare industry has become a prime target for threat actors: “High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks.”⁸

⁷ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

⁸ *The healthcare industry is at risk*, <https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/>

52. Additionally, healthcare providers “store an incredible amount of patient data. Confidential data that’s worth a lot of money to hackers who can sell it quickly – making the industry a growing target.”⁹

53. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, a healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.¹⁰

54. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

55. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹¹

⁹ *Id.*

¹⁰ 2022 Breach Barometer, <https://www.protenus.com/breach-barometer-report>.

¹¹ https://www.law360.com/patientprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=patientprotection

56. As companies became more dependent on computer systems to run their business,¹² the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹³

57. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

58. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

59. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

60. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

61. As a healthcare entity in custody of the Private Information of its patients, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data

¹² <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

¹³ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

D. The Data Breach Was Preventable.

62. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

63. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing Private Information.

64. As explained by the FBI, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹⁴

65. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

¹⁴ How to Protect Your Networks from RANSOMWARE, at 3, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁵

66. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-Facing Assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

¹⁵ *Id.* at 3-4.

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁶

67. Given that Defendant was storing the Private Information of its current and former patients, Defendant could and should have implemented the above measures to prevent and detect cyberattacks.

68. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of more than eight hundred thousand individuals, including that of Plaintiffs and Class Members.

¹⁶ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020) <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

E. Defendant Fails To Comply With FTC Guidelines.

69. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 (“FTC Act”) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act.

70. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁷ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁸

71. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

72. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

¹⁷ 17 C.F.R. § 248.201 (2013).

¹⁸ *Id.*

understand their network's vulnerabilities; and implement policies to correct any security problems.¹⁹

73. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²⁰

74. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. These FTC enforcement actions include actions against healthcare entities, like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (Henry Ford) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that

¹⁹ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

²⁰ *Id.*

LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

77. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information of its patients or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

78. Defendant was at all times fully aware of its obligation to protect the Private Information of its patients, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

F. Defendant Fails To Comply With HIPAA Guidelines.

79. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

80. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).²¹ See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

81. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

²¹ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining PHI. HITECH references and incorporates HIPAA.

82. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

83. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

84. "Electronic protected health information" is "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

85. Under C.F.R. 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) "with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

86. HIPAA requires Defendant to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted and
- d. Ensure compliance by its workforce.

87. HIPAA also requires Defendant to “review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e).

88. Additionally, Defendant is required under HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

89. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against use or disclosure of electronic PHI that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

90. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*”²²

91. HIPAA requires a covered entity to have and apply appropriate sanctions against patients of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

92. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

²² Breach Notification Rule, U.S. Dep’t of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

93. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318.

94. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e- and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material.²³ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-.” US Department of Health & Human Services, Guidance on Risk Analysis.²⁴

95. Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiffs’ and Class Members’ PHI that it receives and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

96. Given the application of HIPAA to Defendant, and that Plaintiffs and Class Members entrusted their PHI to Defendant to receive healthcare services, Plaintiffs and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

²³ <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

²⁴ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

G. *Defendant Fails To Comply With Industry Standards.*

97. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data.

98. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

99. Other best cybersecurity practices that are standard for healthcare entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

100. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

101. These foregoing frameworks are existing and applicable industry standards for healthcare entities, and upon information and belief, Defendant failed to comply with at least one

or all of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

H. The Value of Plaintiffs' & Class Members' Private Information.

102. As a result of Defendant's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information.

103. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.²⁵

104. For example, personal information can be sold at a price ranging from \$40 to \$200.²⁶ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁷

105. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "[m]edical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from \$20 say up to—we've even seen \$60 or \$70."²⁸

²⁵ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

²⁶ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

²⁷ *In the Dark*, VPNOverview, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

²⁸ *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, New Ponemon Study Shows, IDX (May 14, 2015), <https://www.idexpertsCorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat>

106. A complete identity theft kit that includes health insurance credentials may be worth up to \$1,000 on the black market whereas stolen payment card information sells for about \$1.²⁹ According to Experian:

Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.

ID theft victims often have to spend money to fix problems related to having their data stolen, which averages \$600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly \$13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.

Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.³⁰

107. Moreover, Social Security numbers, which, upon information and belief, were compromised for some Class Members in the Data Breach, are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

²⁹ *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, <https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>

³⁰ Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>

108. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases."³¹ Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."³²

109. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.³³

110. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."³⁴ "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."³⁵

³¹ <https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.>

³² *Id.*

³³ Social Security Administration, *Identity Theft and Your Social Security Number* <https://www.ssa.gov/pubs/EN-05-10064.pdf>

³⁴ See <https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/>

³⁵ See <https://www.investopedia.com/terms/s/ssn.asp>

111. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

112. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."³⁶

113. Identity thieves can use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

114. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *See, e.g., Portier v. NEO Tech. Sols.*, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."); *McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021)

³⁶ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>

(noting that Social Security numbers are arguably “the most dangerous type of personal information in the hands of identity thieves”).

115. Similarly, the California state government warns patients that: “[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job.”³⁷

116. Driver’s license numbers, which were compromised in the Data Breach, are incredibly valuable. “Hackers harvest license numbers because they’re a very valuable piece of information.”³⁸

117. A driver’s license can be a critical part of a fraudulent, synthetic identity—which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200.³⁹

118. According to national credit bureau Experian:

A driver’s license is an identity thief’s paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver’s license number, it is also concerning because it’s connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver’s license on file), doctor’s office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver’s license number is one of the most important pieces of information to keep safe from thieves.

³⁷ See <https://oag.ca.gov/idtheft/facts/your-ssn>

³⁸ *Hackers Stole Customers’ License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658>.

³⁹ <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658>.

119. According to cybersecurity specialty publication CPO Magazine, “[t]o those unfamiliar with the world of fraud, driver’s license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation.”⁴⁰

120. However, this is not the case. As cybersecurity experts point out, “[i]t’s a gold mine for hackers. With a driver’s license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification or use the information to craft curated social engineering phishing attacks.”⁴¹

121. Victims of driver’s license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.⁴²

122. Theft of PHI, which, upon information and belief, was compromised in the Data Breach, is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”⁴³

123. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.*, patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to

⁴⁰ <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/>.

⁴¹ *Id.*

⁴² *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021, <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html>.

⁴³ *Medical I.D. Theft, EFraudPrevention* <https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected>.

cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

124. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.⁴⁴ Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.⁴⁵ In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.⁴⁶

125. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.⁴⁷

126. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."⁴⁸

⁴⁴ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/>.

⁴⁵ <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/>

⁴⁶ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/>

⁴⁷ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>

⁴⁸ Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>.

127. A study by Experian found that the average cost of medical identity theft is “about \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.⁴⁹ Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.⁵⁰

128. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

129. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”⁵¹

130. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

⁴⁹ See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar, 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>.

⁵⁰ *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>.

⁵¹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

131. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used.

132. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁵²

133. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses previously obtained PII and PHI about an individual, such as their name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information

134. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

I. Common Injuries & Damages.

135. As a result of Defendant’s ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages,

⁵² *Report to Congressional Requesters*, GAO, at 29 (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf>

including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

J. Data Breaches Increase Victims' Risk Of Identity Theft.

136. As Plaintiffs have already experienced, the unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

137. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

138. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

139. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used

in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

140. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"⁵³

141. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective patients."⁵⁴

142. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a patient's identity after the initial account setup[.]"⁵⁵

⁵³ See N.C. Gen. Stat. § 132-1.10(1).

⁵⁴ See <https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers>

⁵⁵ See <https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/>

143. Since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"⁵⁶

144. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.⁵⁷

145. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

146. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still

⁵⁶ See <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>

⁵⁷ "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-1/>(<https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/>)

easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

147. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like insurance information) of Plaintiffs and the other Class Members.

148. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

149. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

K. Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

150. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the resource and asset of time has been lost.

151. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Online Notice instructs Plaintiffs and Class Members to take the following measures to protect themselves: “remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits, and free credit reports for unexpected activity and to detect errors.”⁵⁸

⁵⁸ See Online Notice, *supra* note 6.

152. In addition, Defendant’s Notice letter includes a full two pages devoted to “Steps You Can Take to Protect Personal Information” that recommend Plaintiffs and Class Members to partake in activities such monitoring their financial accounts, placing fraud alerts on their accounts, and contacting government agencies.⁵⁹

153. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, changing passwords, and monitoring their financial accounts for any unusual activity, which may take years to detect. Accordingly, the Data Breach has caused Plaintiffs and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

154. Plaintiffs’ mitigation efforts are consistent with the 2007 GAO Report regarding data breaches which noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”⁶⁰

155. Plaintiffs’ mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.⁶¹

⁵⁹ *Id.*

⁶⁰ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

⁶¹ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

L. Diminution of Value of Private Information.

156. PII and PHI are valuable property rights.⁶²

157. Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

158. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.⁶³

159. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁶⁴

160. In fact, the data marketplace is so sophisticated that patients can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{65,66}

161. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁶⁷

⁶² See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf>.

⁶³ See, e.g., John T. Soma, *et al.*, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“Private Information”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

⁶⁴ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

⁶⁵ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

⁶⁶ <https://datacoup.com/>

⁶⁷ <https://digi.me/what-is-digime/>

162. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”⁶⁸

163. As a result of the Data Breach, Plaintiffs’ and Class Members’ Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

164. Here, where health insurance information was among the Private Information impacted in the Data Breach, Plaintiffs’ and Class Members’ risk of suffering future medical identity theft is especially substantial.

165. Indeed, “there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII.”⁶⁹ For example,

⁶⁸ *Medical I.D. Theft*, EFraudPrevention
<https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.>

⁶⁹ *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report, at 35-38 (Dec. 2010), <https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework>.

different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.⁷⁰

166. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

167. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to more than eight hundred thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

168. Upon information and good faith belief, had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented the ransomware attack into their systems and, ultimately, the theft of the Private Information of patients within their systems.

169. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

M. Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary.

170. Given the type of targeted attack in this case, sophisticated criminal activity, the type of Private Information involved, and Plaintiffs' Private Information already being disseminated on the dark web, there is a strong probability that entire batches of stolen information

⁷⁰ See *id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money, file false tax returns, take out loans or lines of credit, or file false unemployment claims.

171. The fraudulent activity resulting from the Data Breach may not come to light for years. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.⁷¹ This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.⁷²

172. For example, such fraud may go undetected until debt collection calls commence months or even years later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

173. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

174. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

⁷¹ See *Medical ID Theft Checklist*, <https://www.identityforce.com/blog/medical-id-theft-checklist-2>

⁷² *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches* (Apr. 2010), <https://www.experian.com/innovation/thought-leadership/medical-identity-theft-healthcare-data-breaches.jsp>

175. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

N. Plaintiffs & Class Members Have Suffered Compensable Damages.

176. Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways.

177. The risks associated with identity theft, including medical identity theft, are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

178. In order to mitigate against the risks of identity theft and fraud, Plaintiffs and Class Members must devote time, energy, and money to (i) closely monitor their medical statements, bills, records, and credit and financial accounts; (ii) change login and password information on any sensitive account even more frequently than they already do; (iii) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (iv) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

179. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

180. Further, the value of Plaintiffs and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

181. Plaintiffs and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

182. Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

183. Plaintiffs and Class Members also did not receive the full benefit of their bargain when paying for medical services. Instead, they received services of a diminished value to those described in their agreements with Defendant. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

184. Plaintiffs and Class Members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

185. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

PLAINTIFFS' EXPERIENCE

A. Plaintiff Kirkston Spann II

186. Plaintiff Kirkston Spann II is a former patient of Defendant who obtained services there in or about 2023.

187. As a condition of obtaining services at Defendant, he was required to provide his Private Information to Defendant.

188. At the time of the Data Breach—May 15, 2023 through May 23, 2023—Defendant maintained Plaintiff's Private Information in its system.

189. Plaintiff Spann II is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

190. Upon information and belief, Plaintiff's Private Information was compromised in the Data Breach.

191. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, changing passwords, and monitoring his financial accounts for any unusual activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

192. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his

Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

193. Plaintiff additionally suffered actual injury in the form of his Private Information being disseminated on the dark web, according to Credit Karma, which, upon information and belief, was caused by the Data Breach.

194. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

195. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

196. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

197. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

198. Plaintiff Kirkston Spann II has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

B. Plaintiff Rochelle Lampkin

199. Plaintiff Rochelle Lampkin is a patient of Defendant who started to use Defendant's services in early 2023.

200. As a condition of obtaining services from Defendant, she was required to provide her Private Information to Defendant.

201. Upon information and good faith belief, Defendant maintained Plaintiff's Private Information in its systems at the time of the Data Breach.

202. Plaintiff Lampkin is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

203. Upon information and belief, Plaintiff's Private Information was compromised in the Data Breach.

204. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring her financial accounts for any unusual activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

205. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

206. Plaintiff additionally suffered actual injury in the form of her Private Information being disseminated, on information and belief, on the dark web as a result of the Data Breach.

207. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

208. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

209. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

210. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

211. Plaintiff Lampkin has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

212. Plaintiffs bring this class action on behalf of themselves and all other individuals who are similarly situated pursuant to Pursuant to Rules 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5).

213. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

Nationwide Class

All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach that occurred within Defendant's computers systems in May 2023 (the "Nationwide Class").

Michigan Subclass

All individuals residing in the State of Michigan whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach that occurred within Defendant's computers systems in May 2023 (the "Michigan Subclass").

214. The Nationwide Class and Michigan Subclass are collectively referred to as the Class.

215. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family patients.

216. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

217. **Numerosity:** The patients of the Class are so numerous that joinder of all patients is impracticable, if not completely impossible. According to the breach report submitted to the Office of the U.S. Department of Health and Human Services, approximately 858,238 persons were impacted in the Data Breach.⁷³ The Class is identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

218. **Commonality & Predominance:** Common questions of law and fact exist as to all Class Members and predominate over any questions affecting solely individual patients of the Class. Questions of law and fact common to the Class that predominate over questions which may affect individual Class Members include the following:

- a. Whether Defendant failed to timely notify Plaintiffs and Class Members of the Data Breach;
- b. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;
- c. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;
- d. Whether Defendant had respective duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;
- e. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;
- f. Whether and when Defendant actually learned of the Data Breach;

⁷³ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

- g. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;
- h. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;
- i. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- k. Whether Defendant were unjustly enriched;
- l. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;
- m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

219. **Typicality:** Plaintiffs' claims are typical of those of the other patients of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other patient of the Class.

220. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members

uniformly and Plaintiffs' challenges of these policies hinge on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

221. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members. Plaintiffs have also retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

222. **Superiority and Manageability:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

223. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof

of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

224. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

225. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

226. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

227. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

228. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely notify Plaintiffs and the class of the Data Breach;

- b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard patient Private Information; and
- f. Whether adherence to FTC data security recommendations and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On Behalf of Plaintiffs & the Class)

229. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

230. Defendant requires its patients, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

231. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

232. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

233. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

234. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

235. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

236. By voluntarily undertaking and assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

237. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

238. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or

disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes PHI within the meaning of HIPAA.

239. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiffs or Class Members of the Data Breach until June 2024 despite, upon information and belief, Defendant knowing shortly after May 23, 2023 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiffs and the Class.

240. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein and to ensure that its systems and networks adequately protected their Private Information.

241. Defendant’s duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of being patients at Defendant.

242. Defendant’s duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

243. Defendant was subject to an “independent duty,” untethered to any contract between Defendant and Plaintiffs or the Class.

244. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients’ Private Information it was no longer required to retain pursuant to regulations.

245. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

246. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

247. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Allowing unauthorized access to Class Members' Private Information;
- d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- e. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations, and
- f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

248. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

249. Plaintiffs and Class Members were within the class of persons the FTC Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statutes were intended to guard against.

250. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

251. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

252. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

253. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

254. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

255. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems or transmitted through third party systems.

256. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

257. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

258. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class because of the Data Breach.

259. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

260. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

261. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

262. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or

risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

263. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs' Private Information being disseminated on the dark web; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

264. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

265. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

266. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II

BREACH OF IMPLIED CONTRACT (On Behalf of Plaintiffs & the Class)

267. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

268. Plaintiffs and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining services from Defendant. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

269. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

270. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing medical products and/or services to Plaintiffs and Class Members.

271. Plaintiffs and the Class entrusted their Private Information to Defendant. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

272. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including HIPAA and FTC guidelines on data security) and were consistent with industry standards.

273. Implicit in the agreement between Plaintiffs and Class Members and Defendant to provide Private Information, was the latter's obligation to: (a) use their Private Information for business purposes only, (b) take reasonable steps to safeguard their Private Information, (c) prevent unauthorized disclosures of their Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or use, and (f) retain their Private Information only under conditions that kept it secure and confidential.

274. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

275. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

276. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

277. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

278. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

279. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

280. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

281. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

282. Every contract in Illinois has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

283. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal

information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

284. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs' Private Information being disseminated on the dark web; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

285. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

286. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures, (ii) submit to future annual audits of its systems and monitoring procedures, and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III

**BREACH OF FIDUCIARY DUTY
*(On Behalf of Plaintiffs & the Class)***

287. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

288. In light of the relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became the guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information to act primarily for Plaintiffs and Class Members, (i) for the safeguarding of Plaintiffs' and Class Members' Private Information, (ii) to timely notify Plaintiffs and Class Members of a data breach and disclosure, and (iii) to maintain complete and accurate records of what information (and where) Defendant previously stored and continues to store.

289. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its current and former patients—in particular, to keep their Private Information secure.

290. Because of the highly sensitive nature of the PII and/or PHI, Plaintiffs and Class Members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

291. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

292. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

293. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

294. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

295. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs' Private Information being disseminated on the dark web; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

296. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV

**VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND
DECEPTIVE BUSINESS PRACTICES ACT
815 ILCS 505/2, et seq.
*(On behalf of Plaintiffs & the Class)***

297. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

298. Defendant offered and continues to offer healthcare and other related services in the State of Illinois.

299. Defendant's principal place of business is located in the State of Illinois.

300. Decisions surrounding Defendant's security protocols and response to the Data Breach likely occurred or originated from the State of Illinois.

301. Plaintiffs and Class Members purchased and received healthcare or other services from Defendant for personal, family, or household purposes.

302. Defendant engaged in unlawful and unfair practices in violation of the ICFA by failing to, or contracting with companies that failed to, implement and maintain reasonable security measures to protect and secure Plaintiffs' and Class Members' Private Information in a manner that complied with applicable laws, regulations, and industry standards.

303. Defendant makes explicit statements to their patients that their Private Information will remain secure and private.

304. Defendants' duties also arise from the Illinois Personal Information Protection Act ("PIPA"), 815 ILCS 530/45(a) which requires: "[a] data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to

protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.”

305. Upon information and good faith belief, numerous Class Members are residents of the state of Illinois.

306. Defendant violated its duty under PIPA by failing to, or contracting with companies that failed to, implement reasonably secure data security policies.

307. PIPA requires entities that experience a data breach to notify Illinois residents “in the most expedient time possible and without unreasonable delay.” 815 ILCS 530/10.

308. A violation of PIPA constitutes an unlawful practice under the ICFA. *See* 815 ILCS 530/20.

309. Defendant further violated the ICFA by failing to notify its current and former patients of the Data Breach in a timely manner.

310. Due to the Data Breach, Plaintiffs and Class Members have lost property in the form of their Private Information.

311. Further, Defendant’s failure to adopt, or contracting with companies that failed to adopt, reasonable practices in protecting and safeguarding their patients’ Private Information will force Plaintiffs and Class Members to spend time or money to protect against identity theft.

312. Plaintiffs and Class Members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendant’s practice of collecting and storing Private Information without appropriate and reasonable safeguards to protect such information.

313. As a result of Defendant’s violations of the ICFA, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) invasion of

privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs' Private Information being disseminated on the dark web; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

COUNT V

VIOLATION OF THE MICHIGAN CONSUMER PROTECTION ACT Mich. Comp. Laws Ann. § 445.901, *et seq.* (On behalf of Plaintiff Rochelle Lampkin & the Michigan Subclass)

314. Plaintiff Rochelle Lampkin re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

315. Defendant is required to accurately and notify Plaintiff Lampkin and the Michigan Subclass when it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted personal information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

316. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Mich. Comp. Laws Ann. § 445.72(1).

317. Plaintiff Lampkin's and the Michigan Subclass' Private Information as defined in the Complaint (*e.g.*, Social Security numbers) includes personal information as covered under Mich. Comp. Laws Ann. § 445.72(1).

318. Because Defendant discovered a security breach and had notice of a security breach (where unencrypted and unredacted personal information was accessed or acquired by unauthorized persons), Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

319. Defendant has stated that the Data Breach occurred on or about May 2023 and that it immediately began an extensive investigation to determine what happened.

320. Defendant has also stated that in June 2023, the investigation determined that an unauthorized actor copied certain files from the network between May 15 and May 23, 2023.

321. However, Defendant did not notify Plaintiff Lampkin and the Michigan Subclass until approximately May 2024, approximately eleven months after it discovered the Data Breach and a year after it confirmed that Private Information had been compromised.

322. As a direct and proximate result of Defendant's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff Lampkin and the Michigan Subclass suffered damages as set forth herein.

323. Plaintiff Lampkin and the Michigan Subclass seek relief under Mich. Comp. Laws Ann. § 445.72(13), including, but not limited to, a civil fine of up to \$250 for each violation.

COUNT VI

Unjust Enrichment (On Behalf of Plaintiffs & the Class)

324. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

325. Plaintiffs bring this Count in the alternative to their breach of implied contract claim above.

326. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid Defendant and/or its agents for the provision of services and in so doing also provided Defendant with their Private Information.

327. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

328. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

329. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

330. Defendant acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

331. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information at Defendant or obtained services at Defendant.

332. Plaintiffs and Class Members have no adequate remedy at law.

333. Upon information and belief, Defendant funded its data security measures from its general revenue including payments made by or on behalf of Plaintiffs and Class Members.

334. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

335. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

336. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs' Private Information being disseminated on the dark web; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

337. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Kirkston Spann II and Rochelle Lampkin, on behalf of themselves and all others similarly situated, respectfully request that judgment be entered in their favor and against Defendant Superior Air-Ground Ambulance Service, Inc. and that the Court grant the following:

- A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

- iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiffs' and Class Members' respective lifetimes;
- v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;
- vi. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;
- vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;
- xi. requiring Defendant to conduct regular database scanning and securing checks;
- xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
- xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees'

compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

- xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
 - xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect himself;
 - xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
 - xviii. for a period of ten years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;
 - E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
 - F. For prejudgment interest on all amounts awarded; and
 - G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: August 7, 2024

Respectfully Submitted,

By: /s/ Gary M. Klinger
Gary M. Klinger
**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Phone: (866) 252-0878
gklinger@milberg.com

David S. Almeida (ARDC 6285557)
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
Phone: (312) 576-3024
david@almeidalawgroup.com

Interim Co-lead Counsel

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on August 7, 2024 the foregoing document was filed via the Court's ECF system, which will cause a true and correct copy of the same to be served electronically on all ECF-registered counsel of record.

/s/ Gary M. Klinger
Gary M. Klinger